Alert: Expect a Flood of Hurricane Phishing and Fraud	**Cyber Alert**
Criticality:Green:Low/Informational	**9/03/2019**

Summary	• Malicious actors are taking advantage of Hurricane Dorian to send out phishing scams and fraudulent charity requests. • All computer users should be aware of and avoid these scams.
Criticality	Criticality is ***low/informational***, based on current events.
Warning	Major events, like Hurricane Dorian, mass tragedies, big sporting events, and celebrity happenings, tend to attract malicious individuals who use the events for their gain. Internet watch groups and cyber security experts have already identified multiple fake domains/websites and charity efforts taking advantage of Hurricane Dorian. Stay vigilant: • Be especially cautious of emails, social media, and websites that claim to provide new, sensational information, pictures, or video because they may contain malicious software, and • Be wary of emails and social media asking you to donate to charities. The charities may be fraudulent, and the provided links may go to spoofed charity websites.
Common Scams	Common scams and malicious messages include • Fake Facebook and Go Fund Me pages • Fake charities • Tweets requesting charity donations • Phishing emails pretending to come from animal shelters and religious organizations, and • Malicious emails promising shocking, sensational pictures or video.
Hallmarks of Phishing Scams	Listed below are a few indicators that an email may be a phishing scam. • **Unofficial "From" address**. Look for a sender's email address doesn't come from the organization or that is similar to, but not the same as the organization's official email address, such as redcrooss.org instead of redcross.org. • **Urgent action required**. Be wary of emails requiring you to act immediately. If you don't act now, some dire action will occur or you'll lose out on a great opportunity. • **Requests for personal information**. Legitimate companies do not ask you to verify or provide confidential information in an unsolicited email. • **Wrong look and feel**. While the "quality" of phishing scams has improved, many still come with spelling errors, poor grammar, and poor graphics.
To Verify Charities	You can check out charities with give.org, the Better Business Bureau's (BBB) Wise Giving Alliance.

Hallmarks of Fake Charity Requests	According to the BBB, here are additional reminders to ensure your donation goes to legitimate charities. • **Don't fall for copycats**. Double-check the name of charities. A scammer may use a copycat name that is similar to a reputable organization. • **Don't provide sensitive personal information**. Legitimate charities do not ask for your social security number or driver's license information, although you may need to provide your credit card information if that's how you're donating. • **Beware of high-pressure, urgent demands**. Legitimate charities are glad to accept a donation later.
To Report Suspicious Activity	Please report potential, suspected, and/or confirmed cyber threats to the ACTIC. Provide known or suspected • Threat/attack method • Indicators of compromise • Adversary(ies) • Impact, and • Any other threat actor characteristics. Note: The ACTIC shares victims' applicable critical infrastructure sector and scale of operations (national, regional, state, or local level). ***The ACTIC does not share any identifying information without the victim's consent.*** Please report suspicious activity to the ACTIC via: • http://www.azactic.gov/Tips/ • ACTIC@AZDPS.GOV • (602)644-5805 or (877) 2 S A V E A Z (272- 8329)
Disclaimer	This alert is provided for your situational awareness to help improve Arizona's cyber resiliency. While this document may mention vendors' products and services, the ACTIC does not recommend or endorse any specific ones.